Amendment to the Claims:

This listing of claims will replace all versions, and listings, of claims in the application:

Listing of Claims:

Claims 1-30 (Canceled)

31. (New) A method of reducing handoff latency of a mobile node (MN) roaming between access points in a wireless network (WLAN), the method comprising:

authenticating the mobile node (MN) with an access point (AP) to produce a pairwise master key (PMK);

establishing a pairwise transient key (PTK) as a link layer session key to provide secure communication of 802.1X messages and 802.11 data between the mobile node and the access point;

associating the mobile node with the access point disposed on said wireless network, wherein said associating includes issuing an association request by said mobile node to the access point including signature information indicative of the mobile node holding a fresh/live pairwise transient key;

validating the signature information by the access point;

delivering a protected group transient key (GTK) from the access point to the mobile node, the group transient key being used to protect broadcast communication of the access point comprising generating an association response to send to the MN containing an encrypted field protecting the GTK and including signature information indicative of the AP holding the same fresh/live key PTK as the MN;

validating the signature information by the MN and storing the encrypted GTK for use in multicast communications by the AP; and

forwarding a re-association confirmation message from the mobile node MN to the access point AP to confirm receipt of the group transient key GTK by the mobile node MN;

wherein said establishing establishes said pairwise transient key PTK before said associating is initiated;

wherein said issuing the re-association request by the mobile node MN includes issuing a resuscitation request as Authenticate PTK (SRandom, PTKID MIC);

wherein said validating and said delivering includes delivering a re-association response from the access point AP to the mobile node MN as Authenticate PTK (ARandom, SRandom, PTKID, GTK, GTKID, MIC), deliver encrypted group key; and,

wherein said forwarding the re-association confirmation message includes forwarding a re-association confirm from the mobile node MN to the access point AP as Group Key Confirm (ARandom, MIC).

32. (New) The method according to claim 31 wherein said authenticating and said establishing are initiated before said re-associating.

33. (New) The method according to claim 31 wherein said establishing includes performing an 802.11 4-way handshake to generate said pairwise transient key PMK using said pairwise master key PMK.

34. (New) The method according to claim 31 wherein the authenticating includes:

producing said pairwise master key PMK by at least one of:

retrieving said pairwise master key PMK from a cache memory of said access point AP, and

executing an 802.1X extensible authenticated protocol EAP by the access point AP together with an authentication server AS of said wireless network WLAN to generate said pairwise master key PMK.

35. (New) The method according to claim 31 wherein said authenticating includes negotiating a security association type.

36. (New) In a wireless network (WLAN) including at least one mobile node (MN) roaming between access points of the wireless network, a system for reducing handoff latency, the system comprising:

means for authenticating the mobile node with an access point (AP) to produce a pairwise master key (PMK);

means for establishing a pairwise transient key (PTK) as a link layer session key to provide secure communication of 802.1X compatible messages and 802.11 compatible data between the mobile node and the access point;

means for associating the mobile node with the access point in said wireless network;

means for validating the signature information by the access point; and,

means for delivering a protected group transient key (GTK) from the access point to the mobile node, the group transient key being used to protect broadcast traffic from the access point, the means for delivering comprises means for generating an association response to send to the MN containing an encrypted field protecting the GTK and including signature information indicative of the AP holding the same fresh/live key PTK as the MN;

means for validating the signature information by the MN and storing the encrypted GTK for use in multicast communications by the AP; and

means for forwarding a re-association confirmation message from the mobile node to the access point to confirm receipt of the group transient key by the mobile node;

wherein said means for establishing is adapted to establish said pairwise transient key PTK before said associating means is initiated;

wherein said re-associating means includes means for issuing a re-association request by said mobile node MN to the access point AP including signature information indicative of the mobile node MN holding a fresh/live pairwise transient key PTK;

wherein said means for issuing the re-association request by the mobile node includes means for issuing a resuscitation request as Authenticate PTK (SRandom, PTKID MIC);

wherein said means for validating and said delivering includes means for delivering a re-association response from the access point to the mobile node as Authenticate PTK (ARandom, SRandom, PTKID, GTKID, GTK, MIC), deliver encrypted group key; and

wherein said means for forwarding the re-association confirmation message includes means for forwarding a re-association confirm from the mobile node to the access point as Group Key Confirm (ARandom, MIC).

37. (New) The system according to claim 36 wherein said means for authenticating and said means for establishing are initiated before said means for re-associating.

38. (New) The system according to claim 36 wherein said means for establishing includes means for performing an 802.11 4-way handshake to generate said pairwise transient key PMK using said pairwise master key PMK.

39. (New) The system according to claim 36 wherein the means for authenticating includes:

means for producing said pairwise master key PMK by at least one of:

retrieving said pairwise master key PMK from a cache memory of said access point AP, and

executing an 802.1X extensible authenticated protocol EAP by the access point AP together with an authentication server AS of said wireless network WLAN to generate said pairwise master key PMK.

40. (New) The system according to claim 36 wherein said means for authenticating includes means for negotiating a security association type.

41. (New) An article of manufacture comprising a program storage medium readable by a computer and embodying one or more instructions executable by the computer to perform method steps for executing a command to perform method of reducing handoff latency of a mobile node (MN) roaming between access points in a wireless network (WLAN), the method comprising:

authenticating the mobile node with an access point (AP) to produce a pairwise master key (PMK);

establishing a pairwise transient key (PTK) as a link layer session key to provide secure communication of 802.1X compatible messages and 802.11 compatible data between the mobile node and the access point;

associating the mobile node with the access point in said wireless network;

validating the signature information by the access point AP; and,

delivering a protected group transient key (GTK) from the access point to the mobile node, the group transient key being used to protect communication between the mobile node and the access point, the delivering a protected GTK comprises generating an association response to send to the MN containing an encrypted field protecting the GTK and including signature information indicative of the AP holding the same fresh/live key PTK as the MN;

validating the signature information by the MN and storing the encrypted GTK for use in multicast communications by the AP; and

forwarding a re-association confirmation message from the mobile node to the access point to confirm receipt of the group transient key GTK by the mobile node;

wherein said establishing establishes said pairwise transient key PTK before said associating is initiated;

wherein said re-associating includes issuing a re-association request by said mobile node MN to the access point AP including signature information indicative of the mobile node MN holding a fresh/live pairwise transient key PTK.

wherein said issuing the re-association request by the mobile node includes issuing a resuscitation request as Authenticate PTK (SRandom, PTKID, MIC);

wherein said validating and said delivering includes delivering a re-association response from the access point to the mobile node as Authenticate PTK (ARandom, SRandom, PTKID, GTKID, GTK, MIC), deliver encrypted group key; and

wherein said forwarding the re-association confirmation message includes forwarding a re-association confirm from the mobile node to the access point as Group Key Confirm (ARandom, MIC).

42. (New) The article of manufacture according to claim 41 wherein said authenticating and said establishing are initiated before said re-associating.

43. (New) The article of manufacture according to claim 41 wherein said establishing includes performing an 802.11 compatible 4-way handshake to generate said pairwise transient key using said pairwise master key.

44. (New) The article of manufacture according to claim 41 wherein the authenticating includes:

producing said pairwise master key by at least one of:

retrieving said pairwise master key from a cache memory of said access point, and

executing an 802.1X compatible extensible authenticated protocol EAP by the access point together with an authentication server (AS) of said wireless network to generate said pairwise master key.

45. (New) The article of manufacture according to claim 41 wherein said authenticating includes negotiating a security association type.